What Should We Do if Signal Messenger Gets Blocked?

A proposal and strategy guide to using Delta Chat as a backup

---

https://signal-contingency-plan.info

In the US, Signal is firmly established as the most trustworthy app for secure communication (Signal does not enjoy such popularity in all parts of the world). As such, we will rely on it more and more as the fascists crank the screws. This means that if Signal gets blocked by the feds, whether by network-blocking or by bureaucratic force, we are fucked without a backup plan.

In this zine, we will discuss how Signal might get blocked in the US, why we think Delta Chat is a good backup, and some tips for using Delta Chat strategically under duress. The contents of this zine are an expansion of what's already available online at **https://signal-contingency-plan.info**

We are not security experts, but we are anti-fascist technologists who will make a best effort at informed speculation.

We invite critique of our proposal and discussion of secure comms. Get at us: **signal-contingency-plan@riseup.net**

How is Signal blocked today?

We're gonna get a bit technical in this section, so feel free to skip to *"How might Signal get blocked in the US"* if you'd like. The main takeaway from this section is this: historically, most Signal blocks have relied on the state in question having physical control of the networking infrastructure in that country. This is not currently the case in the US, so if Signal gets blocked here it'll be using different strategies than in China or Iran, for example.

Signal has already been blocked to varying degrees in some countries including Egypt, the UAE, Oman, Qatar, Iran, Cuba, Uzbekistan, Venezuela, Pakistan, Myanmar, China, and Russia.

In 2021, the Open Observatory of Network Interference (OONI) published a blog post summarizing their findings on how Signal is blocked in some countries **[1]**. Here's a summary:

Iran: Blocked on nearly all Iranian AS networks via bidirectional DNS injection.

China: Blocked on nearly all Chinese AS networks via bidirectional DNS injection.

Cuba: Temporarily blocked on the Cuban AS network in 2021 using Deep Packet Inspection (DPI) to force a TCP connection reset during the TLS handshake to Signal backend servers.

Uzbekistan: Blocked on all Uzbek AS networks using DPI to drop all network packets sent to the Signal backend servers.

The strategies that these four countries use to block Signal share one thing: they require the state to physically control the internet infrastructure. In Cuba, there is one telecommunications company and it is run by the government **[2]**. In China, internet service providers (ISPs) seem to be forced by the state to route all traffic leaving the country through three internet exchanges run by the Chinese government **[3]**. In Iran, all traffic is routed through state-controlled telecommunications infrastructure **[4]**. And in Uzbekistan, it seems that a centralized filtering system is implemented by forcing all ISPs to rent bandwidth from the state-monopoly telecommunications provider **[5]**.

In the US, the state does not physically control the internet infrastructure. ISPs and telecom companies operate more-or-less independently, and the US government is not responsible for any of the infrastructure they rely on. In fact the reverse is true – the US government relies on corporate telecoms and tech giants for most of its own network infrastructure.

What's more, internet exchanges (local hubs where ISPs connect their networks together), which are ripe locations for hostile states to begin taking over the internet, are decreasingly important for actual network connectivity in the US. Instead, tech giants like Google and Microsoft simply run fiber directly to each other's privately controlled network infrastructure. Tech giants even run their own undersea cables.

All this means that if Signal is blocked in the US, it won't be through the same mechanisms as in a country like China, where all

traffic exiting the country is *physically* forced to pass through the "Great Firewall."

But the US state has different and arguably more powerful leverage it could use to block or "deplatform" Signal in the US. It has legal leverage based on the fact that Signal and all of its providers are American companies, legally based within American borders, and subject to the whims of the US Department of Justice.

How might Signal get blocked in the US?

The Russian state's current internet censorship project is an informative example of how Signal might be blocked in the US. The Russian state does not physically control the internet infrastructure in Russia, but it manages to implement a vast surveillance and censorship project regardless using law **[6]**. The Russian government requires all ISPs to run monitoring hardware on their networks, maintains a blocklist of all IP addresses and websites that must be blocked nationally, and then holds ISPs legally culpable if they make banned content available to their users. The US government could easily implement a similar system if the DOJ is willing to play ball (they are). They may not even need to roll out monitoring hardware first.

In the case of Signal specifically, the US state has more than just the censorship levers described above. Signal is itself a US-based company, meaning it's fully exposed to the legal and carceral power of an authoritarian US DOJ. The risk exposure is not just Signal though, it's also with all of Signal's infrastructure providers.

A brief explanation of what we mean by Signal's "providers" is necessary. Signal is a secure chat and voice app. Signal the company writes the code for the app, publishes the app in app stores for Android and iOS, and we all download it. In order for those chats and calls to go anywhere though, Signal runs "backend" servers that route the messages and calls to all our

phones. Signal also writes this backend server code, just like they write the code in the app.

What Signal doesn't do is own or have physical access to all the servers that their backend code runs on. In 2025, this is the case for the vast majority of apps and websites we use – the company we know by name (Spotify, Zoom, Eventbrite, Bandcamp, etc.) writes and owns the code, and they run the servers, but Microsoft or Google or Amazon own the servers and have physical access to them, and the company we know by name just rents time on them.

This means that the US government does not have to go after Signal directly in order to block it. The US government can instead try to force Signal's providers to stop routing their traffic, resolving their domains, or hosting their servers. These provider companies are all much bigger and more aligned with the current fascist US state than Signal is. Here's an incomplete breakdown of who Signal's providers are and what they rely on them for:

Google	Backend servers; image, voice, and file uploads; push notifications, and the Android app store
Amazon	Backend servers; image, voice, and file uploads; and a global caching network (Signal uses Cloudfront)
Microsoft	Backend servers; image, voice, and file uploads
Apple	Push notifications, and the iOS app store
Cloudflare	DNS for the "signal.org" domain, all their other domains, and possibly some caching
Markmonitor	Domain name registration (they manage the "signal.org" domain itself, as well as all of Signal's other domains)

Cloudflare is of special note here, because they have a uniquely tight relationship with the US government as the current technical administrators of the ".gov" top-level domain **[7][8]**. It has also been speculated that Cloudflare was already previously facilitating US state surveillance through their widely used "free" global caching product used by tons of apps and websites across the world **[9]**.

Other than the special case of Cloudflare, a fascist US DOJ could try to force Apple and Google to remove the app from the app store, force Markmonitor to turn off the "signal.org" domain, force Microsoft, Google, and Amazon to stop running their backend servers, etc. They could theoretically block or deplatform Signal by leaning on any one of these infrastructure providers that Signal is totally reliant on and which are all totally within the legal purview of the DOJ. If this were to happen, Signal could not quickly move to other providers. They could do it eventually, but not quickly, because Signal operates at a scale that only the very largest providers can support.

This is all to say, *it can happen here*. So what should we do to prepare?

Preparing for Signal outage

Please continue using Signal. At time of writing, there are no indications that Signal is compromised in any way. Signal has earned our trust for a reason. Its primary weakness to fascist control is its centralization and reliance on US infrastructure providers. Our recommendation assumes that readers of this zine are preparing for a Signal outage, not seeking a Signal replacement. We recommend readers download Delta Chat, set up an account, and establish messages with comrades and loved ones. We recommend doing this now and continuing to use Signal as a primary communication tool.

Like Signal, Delta Chat is a messaging app in which messages are *encrypted by default.* Delta Chat uses a subset of the OpenPGP standard for encryption and has undergone multiple independent

security audits **[10]** (if you're familiar with GPG, please know that Delta Chat's PGP implementation is completely unrelated). The default Delta Chat backend server behavior is to delete your messages once they've been received, meaning the data only resides on the devices of you and your homies.

Delta Chat is unique in the ecosystem of encrypted communication platforms for being *decentralized* and using *email protocols* for communication. Anyone can run a backend server, meaning that we ourselves can just make a new server and migrate to it if a government or ISP starts blocking a server that we're using. The use of email protocols to send messages means that a government or ISP can't simply block the entire Delta Chat protocol on the network, without blocking all email on that network. Blocking all email is unprecedented and would probably cause the government and economy to grind to a halt.

Together, these two things make Delta Chat nimble in an unpredictable future, which is exactly what we will need if it comes to that.

Aside from those technical reasons we love Delta Chat, we also endorse it because it is very easy to use, has official apps for every platform, and is made by anti-fascist open source hackers who are embedded in German leftist communities **[11]**.

If you're still not convinced, see the FAQ for Delta Chat **[12]**.

For information about some of Delta Chat's weaknesses and how to mitigate their effects, see the *"If the outage continues"* section later in this zine.

Downloading Delta Chat

Go to https://delta.chat/download

Onboarding to Delta Chat is so easy that we won't even give instructions. Just install it and create an account. Accept all the defaults **[13]**.

To connect with a friend:

- Meet up in person
- Have one person scan the other's Delta Chat QR code (both click/tap the QR code symbol and one selects “Invite” while the other selects “Scan”)
- Send a few messages

That's it, you're connected!

It's possible to get connected by sending a linkified version of the QR code (over Signal of course) rather than scanning in person.

It's important to get connected with friends on Delta Chat before a potential Signal block. Otherwise you won't be able to communicate securely with them until you meet up in person and scan those QR codes. How will you securely plan to meet up without Signal?

When the outage happens

So Cloudflare has just complied with an Executive Order and you’ve just frantically dug this zine out from under a pile of junk mail because your new Signal messages won’t load. What now?

First things first: Don’t panic; use a trusted VPN. In the simplest scenario of an attack on Signal, ISPs are naively blocking traffic to Signal IP addresses. A VPN connection routed through a country which is not blocking Signal could be the easiest resolution to the issue. VPN recommendations are out of scope for this zine; talk to a libertarian technologist.

From here, if the threat to Signal is more substantial then we expect Signal proxies to be booting up about now. You may be able to check Signal’s blog **[14]**, or Fediverse account **[15]**, or a wider social media search of “#SignalProxy” for proxies being run by the Signal Technology Foundation or by volunteer hackers.

You can give the URL of a proxy to the Signal app, by:

On Android
navigate to Signal Settings > Data and Storage > Use proxy
On iOS
navigate to Signal Settings > Privacy > Advanced > Proxy

It may be the case that publicly searchable proxies are under threat. If you think you might be up to running a TLS proxy, we recommend familiarizing yourself a bit before hand by checking out the Signal TLS Proxy repo **[16]**.

This is the scenario in which using Delta Chat to share stable proxies and information about the threat becomes necessary.

If the outage continues

We must contend with the possibility that Signal Messenger is rendered unusable for long periods of time.

The authors of this zine have used Delta Chat and run a Delta Chat backend server for years, and continue to trust and utilize Delta Chat as part of our communications strategies. That being said, there are vulnerabilities to the technology that must be considered when we chat while the State is attacking us. The usage of email protocols under the hood means that Delta Chat leaves some message metadata unencrypted, including the message sender.

Sealed Sender is a part of Signal's protocol that, in simplest terms, encrypts the author of a message **[17]**. A malicious actor with access to Signal's backend servers would be able to determine how many messages a given Signal user was receiving, but would have no way to determine where those messages where arriving from. The same is not true of Delta Chat nor is such a feature planned **[18]**. This means that a malicious actor with access to the Delta Chat server you're using could potentially draw a social graph of accounts that are communicating with each other, and the times they are doing so. This malicious actor would still need access to

unlocked clients (phone/computer with Delta Chat message history) to tie those accounts to specific devices and people.

For long term use, we can mitigate this risk by using throwaway accounts for specific communications on servers optimized for maximum privacy **[19][20]**. There may be unlisted servers being run by trusted comrades in your network already.

Your Delta Chat app is able to maintain numerous profiles and, in the event of a long term Signal outage, you should use this to your advantage. Each profile has independent contact lists, group chat membership, and could be created on a different server. Servers interoperate with each other ensuring that your profile on the flagship German server can still communicate with your homies' running on the server in their basement.

For what it's worth, creating Delta Chat profiles does not require a phone number like it does on Signal.

For extra super security, let's suppose you want to establish a new chat with a friend on a new throwaway profile:

- In a web browser, go to the main website of the server you want to create a profile on
- Generate the new profile by scanning the "Join" QR code or copying the link from the server you're using
- "Create a New Profile" and generate a random username
- Click the QR code on your new profile and click copy link
- Navigate to your old profile and find the chat with your buddy
- Paste the link **instructing them to follow it from a new, throwaway profile they have created** (If you fail to do this step and a server is compromised, the throwaway profile could be connected to your "social graph.")
- Proceed to chat
- Delete your throwaway profile by right-clicking/long pressing it and selecting "Delete Profile"

As always, messaging platforms are only as secure as the devices used to access them. Follow good phone/computer opsec and utilize Delta Chat's disappearing messages feature. Turn this on by:

- Opening a chat
- Clicking the heading for that chat
- Clicking the three dots icon to open the settings for that chat
- Selecting "Disappearing Messages"
- Selecting a time frame for deleting old messages

You can also automatically delete old messages from your device by going to Settings > Chats > Delete Old Messages. This will only remove messages from your device, not the folks you were chatting with.

Final thoughts

We hope it doesn't come to this and that Signal keeps working forever. But anti-fascism requires more than hope, and planning ahead for a future where the state threatens Signal is essential to our survival.

Thanks for reading. You can reach us at **signal-contingency-plan@riseup.net**

🖤

---

[1] https://ooni.org/post/2021-how-signal-private-messenger-blocked-around-the-world/

[2] https://en.wikipedia.org/wiki/Internet_censorship_in_Cuba#State_control_of_telecommunications

[3] https://en.wikipedia.org/wiki/Great_Firewall#Blocking_methods

[4] https://en.wikipedia.org/wiki/Internet_censorship_in_Iran#Methods

[5] https://opennet.net/research/regions/commonwealth-independent-states

[6] https://en.wikipedia.org/wiki/Internet_censorship_in_Russia

[7] https://domainincite.com/28517-verisign-loses-prestige-gov-contract-to-cloudflare

[8] https://www.iana.org/domains/root/db/gov.html

[9] https://www.devever.net/~hl/cloudflare

[10] https://delta.chat/en/help#security-audits

[11] https://chaos.social/@delta

[12] https://delta.chat/en/help

[13] This will create an account on the flagship nine.testrun.org server.

[14] https://signal.org/blog/

[15] https://mastodon.world/@signalapp

[16] https://github.com/signalapp/Signal-TLS-Proxy

[17] https://signal.org/blog/sealed-sender/

[18] https://delta.chat/en/help#sealedsender

[19] Delta Chat sometimes uses the word “relay” to refer to backend servers. They do this to reflect that backend servers must relay information to each other for messages to be passed. They also use this language to reflect that a backend server immediately deletes messages once they’ve been successfully delivered to a single device account.

[20] https://chatmail.at/relays